USAWC STRATEGY RESEARCH PROJECT

INFORMATION IS POWER, USING INFORMATION IS POWERFUL: COMPONENTS OF A NATIONAL INFORMATION STRATEGY

by

Lieutenant Colonel Wayne A. Parks
United States Army

Mr. David W. Cammons
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

United States Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information is Power, Using Information is Powerful Components of a National Information Strategy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Wayne Parks	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**24**	

ABSTRACT

AUTHOR: Parks, Wayne A. LTC.

TITLE: Information is Power, Using Information is Powerful: Components for a National Information Strategy

FORMAT: Strategy Research

DATE: 16 April 2004 PAGES: 20 CLASSIFICATION: Unclassified

The United States (U.S.) finds itself in the midst of the information age without a national security or military strategy that fully support this new environment. Information strategies are present in previous U.S. administrations and military operations extending throughout the country's history. The difficulty is that these strategies are not clearly defined as informational approaches to achieving ends. The current National Security Strategy addresses diplomatic, economic, and military power but does not provide any substantial effort to instill an information campaign into the overall national strategy. The nation will shape the 21st century through effective use of information and information technology.

In this paper, the author explores the idea that information is an integral part of all national strategies and will play a critical part in furthering expansion of democracy to secure liberty and justice for all. The paper first establishes a working definition for information and various strategies. Based on this definition, the paper examines application to modern warfare and potential for the future. It provides historical and business examples of information strategies in order to examine effects and trends that may contribute to current strategies. The paper places emphasis on explaining the common principles of the information element of power and information technology. It describes the future military vision for information superiority and discusses interdependent components of information.

This paper concludes that an information strategy is inextricably linked to a National Security Strategy and is relevant to the continued success of U.S. international diplomatic and economic relations. It offers one potential avenue for meeting the challenges of the information-age environment envisioned in the near future by avoiding traditional military operations and protecting the nation's precious resources. This potential warrants a more in-depth study of future governmental organizations, structures, and information policies.

TABLE OF CONTENTS

Information is a major element of the national power as a ways and means to achieve the national objectives (ends). Information is also a major consideration in the United States (U.S.) Military to achieve the military strategic objectives during operations. These military objectives should be inextricably linked to the national strategy in order to ensure the nation's goals are attained. The current National Security Strategy for the United States clearly addresses three of the prescribed elements of national power directly but not the fourth element of information. The administration must prepare an information strategy in order to deter war and amplify the nation's diplomatic, economic, and military capabilities. This strategy can be formulated from a study of past national strategies, recent business strategies, and future military concepts.

Limited information strategies are present in previous U.S. Administrations extending back throughout the country's history. The difficulty is that these strategies are not clearly defined as informational approaches to achieving ends. The research material for U.S. governmental aims is extremely sparse in determining how past administrations used or developed information strategies. However, businesses continuously analyze the need for information campaigns and tools to project their strategic future. The U.S. Military is also expending a tremendous amount of effort to transform for the information age. The U.S. Administration could learn many lessons from business, the military, and U.S. history in marketing their ideas or objectives to the nation, government organizations, and the world.

This paper explores the idea that information is an integral part of any strategy in the information age and identifies appropriate components of an information strategy for the U.S. It will briefly describe how information is woven into the current National Security Strategy and then how previous administrations have used information as a tool in their security policies. The paper also provides ideas on the way that business and the military incorporate information as concepts to achieve vital leverage in their plans. Finally, the paper offers some elements of a strategy that uses information for a strategic advantage to achieve U.S. interests. The paper consists of three major parts that are titled: Information Strategies, Joint Military Information Strategies, and Components of an Information Strategy.

Part I analyzes the historical perspective of previous administration information strategies and the way business addresses information as part of their strategic plans. Part

II analyzes the future military concepts for information superiority. It describes information superiority in terms of Joint Vision 2020, Transformation Planning Guidance, and Joint Operations Concepts. Part III presents components of an information strategy that are most suitable for the future environment. This part also describes the elements of national power and ways to adjust them for a national strategy. The conclusion summarizes the facts and elements of an information strategy that is inextricably linked to any national strategy. Defining past experiences and describing future ideas for using information is necessary to ensure success for the information age world. The intent of this paper is to stimulate intellectual debate on the future information strategies for the U.S. Administration and U.S. Military.

INFORMATION STRATEGIES

The Bush Administration's National Security Strategy addresses the diplomatic, economic, and military powers as part of a strategy to "further freedom's triumph over all these foes".[1] Diplomacy is demonstrated by the references to strengthening alliances and cooperation with the other main centers of global power.[2] Economic expansion is a main theme through economic growth and expanding the circle of development.[3] Finally, military might appears in the defeat of global terrorism and protection from weapons of mass destruction.[4] There are limited references to information.

Terms used in the National Security Strategy such as assure, dissuade, deter, and information allude to the need for an information strategy without any substantial effort to instill an information campaign. There is an effort in the National Security Strategy to discuss the U.S. Military role in conducting information operations, collecting intelligence information, and public information efforts.[5] These points never expand into a more detailed description of the power of information to achieve domestic, geopolitical, or military goals to secure national or international goals.

A review of past U.S. Administration policies and approaches leads one to believe that information strategies must remain classified or otherwise closely protected to be successful. This may be true of the current administration as well. President Abraham Lincoln was masterful in his manipulation of the printed press during the Civil War to

communicate his intent and promote the Union war effort against the Confederate States. The 20th Century has several examples of public offices, committees, groups, boards, and political directives to provide a direction for informational ways or means in U.S. themes and messages to the global audience. Many of these methods are cloaked in secrecy to properly achieve their aims or to protect the administrations from political or legal liabilities.

Some language used to describe information strategies has a negative connotation with the public. These terms include psychological operations, propaganda, misinformation, or deception. The Committee on Public Information under President Wilson in 1917 used phrases such as, "fight for the minds of men" and "lies had the force of divisions".[6] These phrases might be interpreted by some as propaganda but the real intent was to provide the world a positive portrayal of the U.S. as the country began to expand their aims beyond their own borders. The Reagan administration directed possible counter-propaganda policies against the Soviet Union as an effort to rest the battle of ideas from the "Soviet propaganda machine". In this case, the Reagan Administration policy was an ideological effort to seize the initiative from the Soviets in order to promote peace instead of conflict.[7]

The national security objectives must include a strategy for use of the information environment. However, the current and future administrations must also be wary of achieving the opposite results of an effectual information campaign. They can either learn from past successes such as Abraham Lincoln or the failures of past administrations throughout the 20th Century. Whatever the lessons learned, the final outcome must reflect the realities of the information age.

Business plans (in free market economies like the U.S., Japan, and Australia) have provided experience for the U.S. Government to draw from in order to link information strategies with the corporate strategic vision. There have been many studies performed throughout the past two decades on innovations in information strategies to take advantage of the changing world and the boom in information systems technology. There appears to be a large gap between what the business world and the U.S. government have learned relative to the new information age.

There are many possible objectives for the U.S. Administration to use in developing an information strategy. They must grasp the different aspects of using information as a powerful tool to accomplish the nation's goals. Their are three potential objectives extracted from the business community: the integration of information systems planning with business planning; intercultural communications in globalization; and strategic use of open source information. These examples are only a small sample of the possibilities available to the administration.

In many ways, the U.S. government is congruent with businesses that have a high information intensity of products/services. This is to say that, "…products are information intensive if their selection, purchase, use and maintenance require careful research and thoughtful consideration by the customer".[8] All businesses require a close relationship between the information systems plan and the business plan but this type of organization will likely operate at higher levels of integration between the two plans.[9] Similarly, business leaders need Chief Information Systems Officers (CIO's) that understand technology and the affect on business strategy. This means that top technology positions are generally filled with people that have business backgrounds rather than computer backgrounds.[10] "A misalignment between a firm's competitive strategy and the rank and role of IT leaders may have an adverse effect on firms."[11]

Globalization has brought about a free flow of information between domestic economies and governments. Communication of information and ideas across language and cultural boundaries has been happening for centuries. Today, however, brings greater challenges due to the proliferation of technology available to all nations across the world thus increasing global communications. Europeans and Americans are not concerned with confrontation and conflict in the same manner as the Japanese.[12] Muslims and Christians have many similarities in the Koran and Bible but these two books differ greatly in their interpretation of god and the associated disciples. These cultural and religious differences impact on how communication is received and interpreted by all parties. This means that business managers must build sufficient linguistic competence; learn local values and cultural backgrounds; recognize local needs and adjust accordingly; know the differences in strategic thoughts; and understand the power of information technology. [13]

Open source information is provided and used by many organizations throughout the world. Media reports and a vast array of other reports and documents are available to any individual, government, or business that has access through modern technology. Some businesses use news wire services, web sites, posted speeches and interviews, and interactive conferences to preannounce marketing and business strategies. These are "low-cost means (given the proliferation of information technology) to inform customers, employees, competitors, channel members, investors, industry experts, and observers of the firm's future intentions".[14] This is leading to an ability to shape the environment rather than react to activities after they happen. The use of open source information and mediums contributes to the corporate strategy that will leverage the best practices and resources of any business and government.

The corporate world provides a fertile environment for learning the linkage between information strategies and the strategic vision of the top leadership. The U.S. Administration only needs to commit the resources necessary to transform two decades of business experience into a strategic policy that uses the power of information and information technology to their advantage. The possibilities are endless as is evident by the success of many corporations in the international market.

JOINT MILITARY INFORMATION STRATEGIES

Department of Defense and the U.S. Military are transitioning from the industrial age into the information age and offer key insights toward possible information strategies at the national strategic level. The U.S. Military has already established doctrine for information warfare and is currently developing doctrine for information superiority. The focus for these concepts characterizes the doctrine as information operations, which is synonymous with the previous term of information warfare.[15] Information operations and information warfare are narrowly focused on a few elements where information superiority blends broader components for the information domain. Several Department of Defense and joint military documents set the strategy for operating in this domain while Joint Forces Command is testing the concepts with their experimentation campaign plan. Military concepts provide

foundations to build a strategy when combined with previous administration and business visions.

The military has identified information as a domain congruent with air, land, sea, and space.[16] The major aspect of transforming the U.S. Military is taking advantage of information technology to improve collaboration for improved decision-making. The key element to U.S. Military operations is the ability for commanders to make decisions. The actions associated with the information domain are aimed at actionable, precise, and timely information to aid this decision-making process. Department of Defense Joint Operations Concepts describe their future operational aims as, "To facilitate decision superiority, the Joint Force must gain and maintain information superiority."[17] Information technology and the desire to achieve information superiority are driving the military into the information domain at a rapid pace.

Information Superiority has three elements according to Joint Forces Command's Experimentation Campaign Plan that focuses the force on developing new concepts of warfare for the 21st century in accordance with Joint Vision 2020 (JV2020). These elements are information operations, information systems, and relative/relevant information.[18] The Department of Defense Joint Operations Concepts document projects that information superiority will be continuous rather than focused solely on wartime. The definition includes this passage:

> **"Information Superiority is an imbalance in one's favor in the information domain with respect to an adversary. The power of superiority in the information domain mandates that the United States fight for it as a first priority even before hostilities begin."[19]**

The nature of organizational collaboration as described in JV2020 emphasizes the need to evaluate the impact of information technology on organizations, processes, systems, and tools. Data and information will be in abundance and will be rapidly accessible by all levels of any organization. Decision-making and execution change significantly under these conditions and may cause military leaders to avoid the past concepts for control and emphasize coordination and synchronization. The dispersed nature of smaller forces impacts the structure and training for future combat formations.

Unit cohesion and battlefield psychology may lead to a sense of isolation and greater freedom of action. The idea of human interaction between leaders and those that they lead changes a culture well known to military leadership for centuries. Additionally, the capability of technology will test the endurance of the human since new systems will be able to operate continuously in all conditions. Organizational collaboration becomes distant and without physical human contact in continuous operations.

The first element of information superiority, information operations, is about operating in the information domain but is somewhat limited in breadth and depth. Department of Defense Joint Operations Concepts defines information operations as:

> **"In support of a joint campaign or national strategy, information operations are the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operation security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own. Information operations are a critical enabler to the functions of engagement, protection and C2."[20]**

Information warfare, from joint doctrine, includes other capabilities and activities: communications security, counter deception, physical security, counterintelligence, counter-propaganda, network management, and information security.[21] Enabling elements to information operations are public affairs and civil affairs. Information warfare is simply those information operations conducted during time of crisis or conflict against an adversary.[22]

The second element is information systems, or sometimes referred to as information technology, and is defined by the military as "the equipment and facilities that collect, process, store, display, and disseminate information".[23] Information systems include computers, communications equipment, visual and virtual displays, policies, and procedures associated with equipment and facilities. Computers consist of hardware, software, and databases. Communications systems that are part of the information systems consist of the network components that transmit data and information from one computer to another. The networks may be local or wide-area in order to connect various

computers. Military information systems are generally viewed as being used for command and control. However, information systems are found in much of the combat and combat support equipment as well as enterprise systems in administrative offices of the Department of Defense.

The military systems are intended to be capable of operating in a Joint Military Technical Architecture. The current systems lack interoperability and the ability to participate in a collaborative environment. Future command, control, intelligence, surveillance, reconnaissance, weapons, and logistics systems will meet interoperability and collaborative standards and incorporate IP-based protocols. The configuration standards and protocols established will make the information systems more effective and efficient in a realistic joint war fighting scenario. Something that is changing for the military is for systems to be able to operate in peacetime as they do in war and with agents from organizations in the other national and international elements of power.

The combination of communications and computer components operate in an information domain labeled as an information infrastructure or info-structure for short. This is the area where information systems and information operations meet and is called computer network operations. Computer network operations are broken down into computer network attack, computer network defense, and information assurance. This is the basis for cyber-war. The US Military is developing a global information grid (GIG) as an info-structure to support military information systems. They must also be able to operate in other global, regional, and local infrastructures if their adversaries and partners work within those domains.

Information systems provide the military an ability to automate time-intensive activities and use collaborative environments for parallel rather than sequential planning processes.[24] These collaborative environments use simulations, training information systems, gaming technology, and modeling to process data and information from storage devices and databases. They provide virtual time scenarios to increase awareness and reduce decision-making timelines. A military commander can receive current situation reports and concurrently process the information through modeling and simulations for rapid decisive operations in peacetime or wartime.

The US Military reliance on information technology demands a process that is responsive and adaptive to rapid technological breakthroughs. This reliance also creates vulnerabilities that an adversary can exploit and a complex system that can fail at inopportune times. Information technology changes so rapidly that legacy systems will need the ability to be updated before newer versions are fielded. The vulnerabilities require a system with redundant and proxy components to ensure continuous operations in case of attack or failure.

Information management is the third element of information superiority as defined by joint and service doctrine. The Army defines information management as, "the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision-making."[25] This definition continues by including information systems in the element of information management. As described previously, JV2020 and Joint Forces Command Experimentation Campaign Plans are separating management of information systems from management of information. The author has chosen to use the joint definition for information superiority over any specific service description. However, this Army definition for information management is the best reflection of what the military means by the term.

Relative and relevant information are key and critical to decision-making within the military structure. The military doctrine generally uses the term relevant to delineate this contributor to information superiority. JV2020 uses the term relative as an appropriate descriptor for information management concepts in conjunction with the term relevant. Relevant information is that which is important to the commander and staff during operations and specifically in decision-making. Military commanders also refer to critical information, which is more directly related to decision-making. Important information is used but critical information leads immediately toward commander's decisions. Relative information is connected and dependent data and information that lead to greater understanding, knowledge, decision-making, or execution. This is the often-missing link in managing information in the military. A tremendous amount of effort is placed on relevant information when both relative and relevant information are critical characteristics of information management.

Army publications list intelligence, surveillance, and reconnaissance as a single element instead of relative information. The author's view is that intelligence is relative information about threats and should be included in relative information about other aspects of military operations rather than separate or in place of. Relative information can be defined as timely, fused, and accurate relevant information with the emphasis on fused information.

Network Centric Warfare is a theory being pursued by the Department of Defense as a result of experiences and research gained throughout the 1990's. The idea is to link key elements of an enterprise to create synergy or power from collaboration and synchronized awareness of the environment. The premise behind Network Centric Warfare is based on how the enterprise thinks and organizes itself, as well as the technology linking it together. The Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Cooperative Research Program (CCRP) is an organization funded by the Department of Defense to provide leadership for command and control research. CCRP funded the Center for Advanced Concepts and Technology (ACT) to research national security implications of the information age. Their publications resulted in the military's theoretical foundations for adapting to the information age that is labeled Network Centric Warfare.

Key concepts of this theory are dispersion, knowledge, and effective linking, not simply communications networks. The term networking applies to human, information systems, and organizational interaction. However, a critical aspect is still the communication systems connecting the nodes together. Contemporary military doctrine defines networks as technical communications devices, information systems, and information technology. Network Centric Warfare theories are much more than that and represent the broader concept of an information-enabled organization.[26]

The best military strategy to support the continuous range of the information domain must include a combination of information operations, information management, and information systems management. Information operations and information warfare in the current military doctrine are rather limited and not effective as a complete strategy. The idea of information superiority and Network Centric Warfare are more appropriate strategies that

will use information and information technology to the fullest. The fight for and effective management of relative and relevant information is the most dominant way to support the military element of power. Information technology is the skeleton and DNA of the information domain.[27] The US Military must manage and care for this technological system in order to take advantage of the power and speed realized from its use. The future strategy for the military in the information age must encompass the entire spectrum of the information domain.

COMPONENTS OF AN INFORMATION STRATEGY

U.S. national information strategy is the science and art of employing the communication or reception of knowledge or intelligence power of the U.S. and world partners to afford the maximum support to adopted policies in peace or war. This description combines common elements of information strategies, theories and concepts between past U.S. Administrations, the U.S. Military, and corporate experience. These players have demonstrated the need for perception management in a fair, balanced, and accurate manner to either promote public policy or counter foreign propaganda aimed at U.S. policies. The international business community strictly aimed information strategies at decision-making in the mid to late 1990's but has since expanded their view to a broad interpretation of operating across the entire information domain. The U.S. Military identifies information technology as a way to improve collaboration for improved decision-making yet sees the advantage of expanding their perspective across the entire continuum of information as well. The U.S. could save valuable resources by simply using information as a means to exploit the other components of power. The only way to ensure this theory is to ensure all elements of national power are identified and properly interrelated.

The primary component of an information strategy is the interrelation between all elements of power. The strategy must thread information throughout the other elements as well as achieve objectives only associated with the information domain. The actions to implement national elements of power have information impacts or can use information as an instrument. Information is likely used as a first element to influence policy and perceptions and a nation should have the capability and resources to use the other

elements concurrently or under extreme circumstances when information is not successful. The national elements of power that are primarily taught in the senior U.S. Military educational institutes are limited to four. These include the economic, diplomatic, military, and information elements of power. Others can be classified as elements of power as well and must be considered as part of this component for an information strategy.

David Jablonsky provides the most exhaustive list for determinants of power. He organizes them into two categories of natural and social determinants. This categorization provides a good framework for developing an information strategy. The natural determinants are geography, resources, and population. These determinants are critical for policymakers to understand in order to communicate knowledge and understanding. However, the natural determinants could be combined into a single natural resource element using geography, population, and additional resources as instruments and tools. The social determinants are economic, political, military, psychological, and informational. The psychological determinant is more suited as an objective for information and should be joined with the informational determinant. The informational element would be aimed at the national will, morale, national character, and degree of national integration to account for the psychological aspect of a nation or population. Jablonsky's inclusion of the political determinant is useful as it relates to domestic politics but he doesn't prescribe an element of diplomatic power as related to international relations with state and non-state actors. The author would return this to the theory to complete the ways and means available to a nation.[28]

Technology has played a significant role throughout history but it is not included as a separate element of power. Nations have seen revolutions with technology and used these innovations to wield their power against their neighbors and others throughout the world. It stands to reason that this would also be considered as an essential element to any national strategy. Technology brought the world industrialization, mechanization, and now information. The author would also add this to the elements of national power. The author's complete list for elements of power to interact with information would be natural resources, diplomatic, military, economic, and technological.

Information technology is another component for U.S. information strategy. The info-structure is complex, powerful, and vulnerable. The info-structure spans the globe and is made up of a group of systems, which the scale and potential energy of the relationship is insufficiently known. The existing and future networks, computers, and databases can lessen uncertainty, grow intellectual capital, and persuade the world to support achievement of national interests. The U.S. Administration has already recognized the vulnerabilities associated with technology and published The National Strategy to Secure Cyberspace.[29] Information may be so important to the global society that it can either be a significant asset or an Achilles heel. The disruption in oil supply spurred global recession in the 1970's and the disruption in flow of information may cause the next recession.[30]

The most important characteristic of this component will be cyber security. The National Strategy to Secure Cyberspace for the American society engages and empowers the citizens to secure portions of the public and private infrastructure owned by the public and individuals. This requires coordination between the entire society and focused effort by the federal government, state and local governments, and the private sector. The US would expand this strategy to include their international partners and the new emerging members of the post-cold war society.

The strategy focuses on response, threat reduction, vulnerability reduction, awareness, training, government infrastructure, and international cooperation. The challenge of the strategy is the balance between freedom of access to information and infrastructure protection. Swift identification, information sharing, and remedy development will alleviate any damage caused by malicious attack to civil computer-based systems. Private information security businesses have already begun to build threat identification and protection services for information systems and telecommunications. This, combined with enhanced law enforcement and federal capabilities, can advance the market for more secure technologies. Government can co-opt civilian security companies in promoting awareness and providing cyber security training programs and certifications. The final step in the cyber security strategy requires a policy of international cooperation to facilitate information protection. Securing cyber space for the U.S. and the world is critical for information technology to succeed as the backbone of the information domain.

The complex nature of information technology demands leadership and an organization that understands technology and the affect on national strategy. Just as in business, the government must fill top technology positions with people that have government and business backgrounds rather than just computer backgrounds. The IT staff is just as important as the leadership and requires special capabilities beyond computer knowledge. Hallmark Cards realized that data was buried within their organization and information systems that was difficult to retrieve and use. They established "information guides", translators between information users and the IT staff, to find the right information and compare it across different business units.[31] A strong alignment between the nation's information strategy and the rank and role of the IT organization will have a powerful effect for the nation. Success for the nation requires an organization that manages complexity, power, and protection of the information technology component.

Another component of an information strategy is relative information management. This component combines fusing, sharing, perceiving, influencing, and expressing relevant information for the nation's ends. Volumes of data and information are available to state and non-state actors across the world. This proliferation must be developed or combined into information that creates understanding by the appropriate or selected audience. Information availability is breaking the nation to nation link and is connecting people directly. As businesses learned this past decade, this is redistributing power and the population can know as much about the nation and international issues as the leaders.

An aspect to relative information management is an idea created by U.S. media professionals. In a recent conference held at the U.S. Army War College, many media participants promoted the concept of a fair, accurate, and balanced angle on all reports and stories.[32] The media claims that they are the "Watchdogs" for the people in order to keep the U.S. Government in check. The U.S. form of democracy ensures freedom of expression and the press in the 1st Amendment but sometimes the slant taken is not always fair, accurate, and balanced. The U.S. strategy must assure proper understanding by assisting in this media concept and provide complete, relative, and relevant information is made to the public.

The nation-state will be around for a long time to come but there needs to be an effort to understand many areas of the world where the population views them as artificial and having limited or no legitimacy. The population is a strong and powerful tool, especially in a democracy. The U.S must see the influence of a population and intercultural communications as a key to an information strategy. The strategic thoughts of a nation are not always compatible with that of the population they control or attempt to control. Proliferation of free press and media across the world will provide strategists with relative open source information in order to understand how communication is received and interpreted by all parties. This means that the U.S must build sufficient linguistic competence; learn local values and cultural backgrounds; recognize local needs and adjust accordingly; and know the differences in strategic thoughts. The networking of humans is becoming more efficient and effective so the information strategy must ensure the proper understanding of related and relevant information to assist meeting the nation's goals.

The U.S. information strategy should include three primary components: interrelating information with all other elements of power; managing information technology; and managing relative information. The strategy requires gaining, disseminating, and protecting information through information technology while synchronizing all instruments or tools of information for the nation. It will evaluate the impact of information technology on organizations, processes, systems, and tools. The objectives for an information strategy will provide sustained multi-faceted approaches to improve relations, expand economic growth, build democracies, and build consensus with other main centers of global power. The U.S must avoid the need to control the information domain but emphasize coordination and synchronization by stressing the enterprise and not the system. The U.S. Government must also be able to operate within other global, regional, and local infrastructures if its adversaries and partners work within those and must have an immediate impact and long-lasting enduring effects to achieve domestic, geopolitical, or military goals.

CONCLUSION

The U.S. Administration must develop an information strategy that is inextricably linked to any national strategy. President Bush needs an information advisor that can align the

use of relative information and information technology with the strategic vision of the nation. The advisor must understand the national goals, technology, and the administration's message. The message must include the natural resources, diplomatic, military, economic, and technological elements of power. It must also consider the geography, resources, and population of the environment where the nation plans to operate.

The administration may already possess an information strategy that is classified as secret or confidential. The power of information tends to have the best effect on the unknowing rather than a prepared audience. However, there are advantages to describing the policy in open sources. The policy of providing fair, accurate, and balanced information to the domestic population, government employees, international competitors, other governments, and observers of the country's future intentions should provide the ability to shape the environment. Information technology needs some level of security and standardization to take full advantage of the powerful capabilities it presents for the nation. Finally, the national strategy must portray a strong understanding of varying cultures, in order to fully communicate the true intentions of democracy and democratic idealism.

Information strategies and the information age present a broad set of challenges for the future. This paper can only offer a narrow set of ideas on the concepts of developing information strategy. The ideas presented can assist in developing future organizations, structures, and strategy for the vast amount of unknowns in the information domain. However, the theories need a great deal of refinement and study before the difficult questions of the information age are answered. The intent of this paper is to stimulate the intellectual debate on future approaches that will provide improved strategies for the nation.

WORD COUNT = 5506

ENDNOTES

[1] George W Bush, *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 2002), POTUS introduction.

[2] ibid, Chapters III and VIII.

[3] ibid, Chapters VI and VII.

[4] ibid, Chapters III and V.

[5] ibid, 30-31.

[6] George Creel, *How We Advertised America* (New York: Harper & Bros., 1920), 3-4, 284.

[7] Norman A. Bailey, *The Strategic Plan that Won the Cold War: National Security Decision Directive 75 (*McLean, VA: Potomac Foundation, 1999), 15.

[8] J. Linder and B. Ives, *"Information Intensity: A Framework for Competitive Advantage"*, Working paper, 1988.

[9] SH Teo Thompson and William R. King, "Integration Between Business Planning and Information Systems Planning: An Evolutionary-Contingency Perspective", *Journal of Management Information Systems* 14, no. 1 (Summer 1997): 194.

[10] Jahangir Karimi, Yash P. Gupta,, and Yoni M. Somers, "The Congruence Between a Firm's Competitive Strategy and Information Technology Leader's Rank and Role", *Journal of Management Information Systems* 13, no. 1 (Summer 1996): 64

[11] ibid, 65.

[12] Susumu Yoshida, "Globalization and Issues of Intercultural Communications", *Vital Speecheds of the Day* 68, no. 22 (September 1, 2002): 710-711.

[13] ibid, 711-712.

[14] Roger J. Calatone and Kim E. Schatzel, "Strategic Foretelling: Communication-Based Antecedents to a Firm's Propensity to Preannounce", *Journal of Marketing* 64, no. 1, (January 2000), 17.

[15] Concepts and doctrine in 1998 labeled US Military information concepts as information warfare. This term is being changed to information operations and some speculation is that this term would be more acceptable to the civilian leaders and the population. This paper uses these terms interchangeably where it is appropriate to refer to warfighting or peacetime operations. See Joint Chiefs of Staff Pamphlet, *Information Warfare; A Strategy for Peace…The Decisive Edge in War*, (Washington D.C.: U.S. Chairman of the Joint Chiefs of Staff, 1998).

[16] Department of Defense, United States of America, *Joint Operations Concepts, JCS Version 1.0 for 2003* (Washington D.C.: Office of the Secretary of Defense, 26 September 2003), Secretary's Foreward, 2.

[17] ibid, 14.

[18] The United States Atlantic Command is now called Joint Forces Command. The Joint Experimentation Campaign Plan is the Department of Defense plan to develop and assess innovative concepts. The current experimentation plans are aimed at testing Joint Vision concepts. United States Atlantic Command, *Joint Experimentation Campaign Plan 2000* (Norfolk, VA. 30 September 1999), A-17 and A-22.

[19] Department of Defense, *Joint Operations Concepts*, 14.

[20] ibid, 21.

[21] Joint Chiefs of Staff, *Joint Pub (JP) 3-13, Joint Doctrine for Information Operations* (Washington D.C.: U.S. Joint Chiefs of Staff, 9October 1998), I-10.

[22] ibid, GL-7.

[23] Department of the Army, *FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures* (Washington D.C.: U.S. Department of the Army, November 2003), Glossary-12.

[24] Department of Defense, United States of America, *Transformation Planning Guidance* (Washington D.C.: Office of the Secretary of Defense, April 2003), 7.

[25] Department of Defense, *FM 3-13*, 1-10.

[26] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (Washington D.C.: CCRP Publication Series, February 2000), 88.

[27] ibid, 15.

[28] David Jablonsky, "National Power," in *U.S. Army War College Guide to Strategy*, ed. Joseph R. Cerami and James F. Holcomb, Jr. (Carlisle Barracks, PA: Strategic Studies Institute, 2001), 90-99.

[29] George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, September 2002).

[30] Richard L. Nolan, Connectivity and Control in the Year 2000 and Beyond, *Harvard Business Review on the Business Value of IT*, (Boston, MA: Harvard Business School Publishing, 1999), 213.

[31] ibid, 24

[32] The ideas presented in this paragraph are based on remarks made by several participants participating in an Embedded Media Conference at Carlisle Barracks.

BIBLIOGRAPHY

Alberts, David S., Garstka, John J., and Stein, Frederick P. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington D.C.: CCRP Publication Series, February 2000.

Bailey, Norman A. *The Strategic Plan that Won the Cold War: National Security Decision Directive 75*. McLean, VA: Potomac Foundation, 1999.

Bush, George W. *The National Security Strategy of the United States of America*. Washington, DC: The White House, September 2002.

_____. *The National Strategy to Secure Cyberspace*. Washington, DC: The White House, September 2002.

Calatone, Roger J. and Schatzel, Kim E. "Strategic Foretelling: Communication-Based Antecedents to a Firm's Propensity to Preannounce." *Journal of Marketing* 64, no. 1 (January 2000): 17-30.

Creel, George. *How We Advertised America*. New York: Harper & Bros., 1920.

Jablonsky, David, "National Power." In *US Army War College Guide to Strategy*, ed. Joseph R. Cerami and James F. Holcomb Jr., 87-106. Carlisle Barracks, PA: Strategic Studies Institute, 2001

Karimi, Jahangir, Gupta, Yash P., and Somers, Yoni M., "The Congruence Between a Firm's Competitive Strategy and Information Technology Leader's Rank and Role." *Journal of Management Information Systems* 13, no. 1 (Summer 1996): 63-88.

Linder, J. and Ives, B., "Information Intensity: A Framework for Competitive Advantage." Working paper, 1988.

Nolan, Richard L. Connectivity and Control in the Year 2000 and Beyond. *Harvard Business Review on the Business Value of IT*. Boston, MA: Harvard Business School Publishing, 1999.

Tanous, Stephen M., Lieutenant Colonel, U.S. Army, *Building A Psychological Strategy for the U.S.: Leveraging the Informational Element of National Power*. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, 22 May 2003.

Thompson, SH Teo and King, William R. "Integration Between Business Planning and Information Systems Planning: An Evolutionary-Contingency Perspective." *Journal of Management Information Systems* 14, no. 1 (Summer 1997): 185-214.

U.S. Atlantic Command, *Joint Experimentation Campaign Plan 2000*. Norfolk, VA: U.S. Atlantic Command. 30 September 1999.

U.S. Department of Defense. *Joint Operations Concepts, JCS Version 1.0 for 2003*. Washington D.C.: Office of the Secretary of Defense, 26 September 2003.

_____. *Transformation Planning Guidance*. Washington D.C.: Office of the Secretary of Defense, April 2003.

U.S. Department of the Army. *Information Operations: Doctrine, Tactics, Techniques, and Procedures*. Field Manual 3-13. Washington D.C.: U.S. Department of the Army, November 2003.

U.S. Joint Chiefs of Staff. *Information Warfare; A Strategy for Peace…The Decisive Edge in War*. Pamphlet. Washington D.C.: U.S. Chairman of the Joint Chiefs of Staff, 1998.

_____. *Joint Doctrine for Information Operations*. Joint Pub 3-13. Washington D.C.: U.S. Joint Chiefs of Staff, 9 October 1998.

Yoshida, Susumu. "Globalization and Issues of Intercultural Communications." *Vital Speeches of the Day* 68, no. 22 (September 1, 2002): 708-712.